CRYPTOGRAPHY IN AMATEUR RADIO COMMUNICATIONS

Robert M. Richardson, W4UCH
22 North Lake Drive
Chautauqua Lake, N.Y. 14722

ABSTRACT:

Some fascinating similarities between the art and science of cryptography and the amateur radio avocation, especially in the area of digital communications are discussed.

GENERAL:

Webster's New World Dictionary defines cryptography as: "The art of writing or deciphering messages in code." As such, every U.S. radio amateur is a cryptographer, some willingly and some kicking and screaming. Even the most erstwhile novice or technician class radio amateur is a cryptographer when he studies for the 5 words per minute Morse code examination. Some radio amateurs become so proficient at deciphering Morse that they can carry on a conversation while copying Morse on a typewriter at 20 - 30 words per minute. Some radio amateurs once they pass the code test never want to hear Morse code again. Either approach is perfectly acceptable within the radio amateur fraternity as it is a house of many mansions with room for all kinds with differing interests and differing specialties.

Let's take a look at some of the synonyms used in the cryptography field before we begin to dig deeper. To code a message, regardless of the variety of coding used, we may use any of the following terms in the English language as they all mean virtually the same thing: encrypt, encode, encipher, or in slang, even the term scramble. The opposite function which returns a message to plaintext is of course: decrypting, decoding, deciphering, or descrambling.

BAUDOT CODE:

Moving up the ladder of commonly used amateur radio encryption we have Baudot radioteletype (RTTY) which has roots back to about 1906 in radio prehistory. It is a synchronous 5 bit code. By synchronous we mean that is has start and stop bits in addition to the 5 data bit code. Having a start and stop bit, we may send Baudot RTTY at say 60 speed and if we are a hunt a peck typist, we might only transmit 10 or so words per minute even though each character is transmitted at a 60 speed rate.

ASCII CODE:

The next level of amateur radio RTTY encryption uses the American National Standard Code for Information Interchange, ASCII. It too is a synchronous code with start and stop bits in addition to its 7 data bits and optional 8th parity bit. On the low frequency bands commonly used Baud rates are 110 and 300 with an -equivalent speed in words per minute of 110 and 300 if the transmission is being sent automatically.

PACKET:

On up the amateur radio encryption ladder another step we find our relatively new friend, packet, first implemented on the ham bands by radio amateurs Rouleau and Hodgson in Quebec circa 1979. This relatively new form is the first synchronous amateur radio data communication system. BY synchronous we mean that no start and stop bits are transmitted, only a stream of ones and zeros in each packet. This system was invented in 1957 by IBM's brilliant Robert Donan and was initially called Synchronous Data Link Control, SDLC.

IBM SDLC:

Defining the fundamental concepts of SDLC in one paragraph is a challenge, but here goes. SDLC, those parts used by radio amateurs is an 8 data bit per byte encrypted code. Each packet (or frame) has a unique opening and closing flag byte or bytes that never appear elsewhere in the packet. Between these flags a logical zero is noted by a change from the previous bit received; i.e., if it changed it is a logical zero. If it did not change it is a logical one. In addition, SDLC uses 'zero insertion' between flags to keep the unique flag byte (126 decimal) from ever being repeated, except when it is used to mark a packet (or frame) opening and closing boundary. The SDLC rule is: whenever more than 5 logical ones are to be transmitted between flags, insert a zero = 'zero insertion.' On receiving, 'zero deletion'

is used; i.e., when a logical zero is received after 5 logical ones, delete it. Before the closing flag is sent in a packet (or frame) a 2 byte cyclic redundancy check (CRC) value is calculated and transmitted. Packets may be generated and decoded either by software or hardware depending upon which variety of packet controller you are using. Commonly used packet Baud rates on the VHF bands are 1200 Baud and up, and on the HF bands, 300 Baud.

Ax. 25 PROTOCOL:

Encoding and decoding packets in real time using the software approach is a fascinating challenge for the amateur radio cryptographer. First, the SDLC discipline must be thoroughly understood. Second, generating and/or checking a real time CRC must be understod. Third and last, the protocol being used must be understood. The latter is probably the most challenging, but with the excellent ARRL book delineating the AX.25 protocol is not all that difficult.

DIGITAL AUDIO ENCODING:

The newest kid on the block, after companded SSB, is digital audio. It will come to pass for the amateur radio fraternity in due course. The' single sideband enthusiasts will scream just as loudly as the AM enthusiasts screamed back in the 1950s when SSB was introduced. It makes no never mind as technology progresses with or without the diehards' approval or disapproval.

CRYSTAL BALL GAZING:

Looking into our crystal ball we can see the early digital audio transmission modes using frequency shift keying (FSK) and phase shift keying (PSK) giving way to more efficient binary phase shift keying (BPSK) and quadrature phase shift keying (QPSK), If a radio amateur cryptographer wishes to get his or her feet wet in the digital audio field, the C-band and Ku-band geosynchronous satellites are a good place to start as most every variety of digital audio is being used. A great deal of the digital audio traffic is just plaintext, with no added encryption of any variety being used.

For those radio amateur crytographers who would like a real challenge, there is now encrypted digital audio on the C-band Galaxy I satellite located at 334 degrees west in the Clarke belt. It may be found on channel 19 with a downlink frequency of 4080 MHz and channel 23 with a downlink frequency of 4160 MHz, both with horizontal polarization. Both channels of audio are encrypted using a modified form of the 56 bit key digital encryption standard (DES).

Is it impossible to decipher a DES encrypted digital audio signal? Of course not. It may be difficult, but it is not impossible. Some radio amateur cryptographers have estimated that it would take a dozen super duper Cray maxi-computers 29 days to search through all 72 quadrillion possible keys to decrypt this type of encoded digital audio.
WRONG: They have overlooked two important facets of the problem at hand:
3. The key (though encoded) is transmitted over the air and may be recorded along with the digital audio signal on any video recorder.
2. The plaintext of the encoded digital audio is available to be recorded from any satellite TV receiver with a decoder.

IS IT LEGAL TO RECORD ? ? ?

Of course it is. The master recordings above were made by a paid subscriber to these services.

DES USERS GROUP:

If you are an amateur radio cryptographer and would like to join the DES Users Group that is investigating this fascinating challenge, send a S.A.S.E. to the DES Users Group, Drawer 1065, Chautauqua, NY 14722, for an info sheet. There are no dues at present. The only requirement is an active interest in amateur cryptography. The 1st annual meeting will be held at the Dayton Hamfest, April 25 - 27, 1986.